Abstract

Method of and Apparatus for Modular Multiplication

In a method for modular multiplication using a multiplication look-ahead process for computing a multiplication shift value and a reduction look-ahead process for computing a reduction shift value, a modulus is first transformed into a transformed modulus that is greater than said modulus. The transformation is carried out such that a predetermined fraction of the transformed modulus has a higher-order digit with a first predetermined value that is followed by at least one low-order digit having a second predetermined value. During the iterative working off of the modular multiplication using the multiplication look-ahead process and the reduction look-ahead process, the transformed modulus is utilized so as to obtain at the end of the iteration a transformed result for the modular multiplication. Finally, the transformed result is re-transformed by modular reduction using the original modulus. By means of the transformation according to the invention, iterative working off of the modular multiplication is simplified so that the modular multiplication can be performed faster.

Fig. 1